Network Voting System Standards

Draft - January 25, 2002

A Framework and Specific Recommendations
proposed by

VoteHere, Inc.
3101 Northup Way, Suite 250
Bellevue, WA 98004
(425) 739-2500

Foreword

These proposed standards are based on the conclusions about the general nature of elections, and in particular the nature of computerized elections, as discussed in How to do Elections Right[1], and in more depth beginning with The Metaphysics of Voting.[2]

These standards are based in part on the Voting System Standards produced by the Federal Election Commission[3], on the findings and recommendations of many of the recent studies on Internet Voting, including the California Task Force on Internet Voting[4], the CalTech/MIT Voting Technology Project[5], the NSF-sponsored National Workshop on Internet Voting[6] and on private research efforts at VoteHere. Where specific language has been "borrowed" from other sources, it is clearly referenced.

These standards differ from the FEC Voting System Standards, in two primary ways:

1. *They are based on a model for protecting election integrity and privacy that derives from auditing the election data, rather than election processes; and*
2. *They describe the general objectives and requirements for a network voting system, and offer very few specific "feature-level" requirements. As specific technologies are applied in attempts to meet the high level requirements of these standards, companion information will be developed to help evaluate the details that are applicable based on each specific technology. Further, systems presented for review under these standards and (any companion standards) will first undergo a complete design review and evaluation. The outcome of this first review step determines if the design is logically able to meet the requirements, and provides the necessary details for specific functional review and testing.*

VoteHere, Inc currently retains the copyright in this work. We are generally willing to release ownership of the work to a suitable standards body or industry group should one desire to take on ownership and oversight of this effort.

Although these standards depart from the specific format and organization of the FEC Voting System Standards, the concepts and specific requirements could be incorporated into that effort with relative ease. Similarly, although these standards focus on Network Voting Systems, the concepts and approach are well suited for all electronic voting systems.

---

[1] http://www.votehere.net/perspectives/DoVotingRight.pdf.
[2] http://www.votehere.net/perspectives/MetaphysicsOfVoting.pdf
[3] http://www.fec.gov/pages/vss/vss.html
[4] http://www.ss.ca.gov/executive/ivote/
[5] http://www.vote.caltech.edu/
[6] http://www.internetpolicy.org/research/results.html

Revision History

Release Date	Changes Made
January 22, 2002	Initial Working Draft Release
January 25, 2002	Updated foreword Clarified use of eligible vs. registered voter

Table of Contents

1. Introduction

1.1. Objectives of the Network Voting System Standards

The primary objective for the Network Voting System Standards is to establish an environment and context in which voting systems can be examined to determine which, if any, can be used in binding elections while remaining consistent with general requirements for fairness, accuracy and privacy.

These standards are designed to address the issues that arise for any system that transmits election data over a network. As such, they are intended to be applicable to all such systems, including wireless, Internet, ATM network, interactive TV and any other form of voting system or network technology that is not under the physical and logical control of the election officials at all times.

Specifically, these standards need to:

- define a set of high level requirements for Network Voting Systems;
- define functional requirements for Network Voting Systems; and
- define specific performance standards for Network Voting Systems.

1.2. Document Format and Conventions

All requirements and standards are indicated by the words 'shall' or 'must'. All requirements and standards are further tagged and identified through the use of an id block that looks like this: *[ID]*, where ID is a unique alpha-numeric identifier for that requirement. Every effort will be made to retain the ID associated with a specific requirement across revisions of these standards, which may result in the IDs appearing "out of sequence" as the organization and content of the standards changes over time.

> Throughout the document, discussion blocks appear in this format (in a gray box). These paragraphs are intended to provide background information, examples, or further discussion of options. No statements in the discussion blocks are to be construed or interpreted as requirements separate from or in conflict with the actual requirements as identified in these standards.

1.3. Definitions

1.3.1. Voting System

A Voting System is a total combination of mechanical, electromechanical or electronic equipment, including the software, firmware, and documentation required to program, control, and support the equipment that is used to define ballots; to cast and count votes; to report and/or display election results; and to maintain and produce all audit trail information.[7]

1.3.2. Election Data

Election Data is the information critical to ensuring the fairness and accuracy of the election. It includes the approved Ballot Styles, the voted ballots ("Vote Data"), the results of tabulation and the election audit information. It does not include information leading up to the production and approval of official ballot styles, nor does it include information verifiably and non-destructively derived from tabulation results (e.g., roll-up reports, results breakdown analysis, etc.)

[7] Excerpted from FEC Voting System Standards (VSS), Section 1.5.1

1.3.3. Ballot Style

A Ballot Style is the collection of information about the races, measures and candidates that a particular voter or group of voters votes on. It can also be thought of as the blank ballot that the voter needs to complete in order to cast their vote.

1.3.4. Electronic Voting System

An Electronic Voting System is a Voting System in which the Election Data is recorded, stored and processed as primarily digital information.

> This broad definition of Electronic Voting System is intended to provide a general category of voting system that contains many different sub-classifications, including traditional stand-alone Direct Recording Electronic Voting Systems and Network Voting Systems as defined in the next section. Like the general definition of Voting System above, it is not the intent that any specific system should be categorized only as an Electronic Voting System, but that all such systems should instead be categorized into one of these more detailed classifications.

1.3.5. Network Voting System

An Network Voting System is an Electronic Voting System in which some or all of the Election Data is transmitted over a communication network that is not physically or logically used exclusively for Election Data. The network may be what is generally considered 'public' (e.g. the Internet) or 'private' (e.g., the ATM banking network).

There are several meaningful sub-categories within the broad classification of Network Voting System:

- *Attended Network Voting Systems*. An Attended Network Voting System is one where the steps of voter identification, authentication and vote casting take place in person, in an environment that is closely controlled and monitored (attended) by election officials. Once cast, the ballots leave the controlled environment via the communication network.

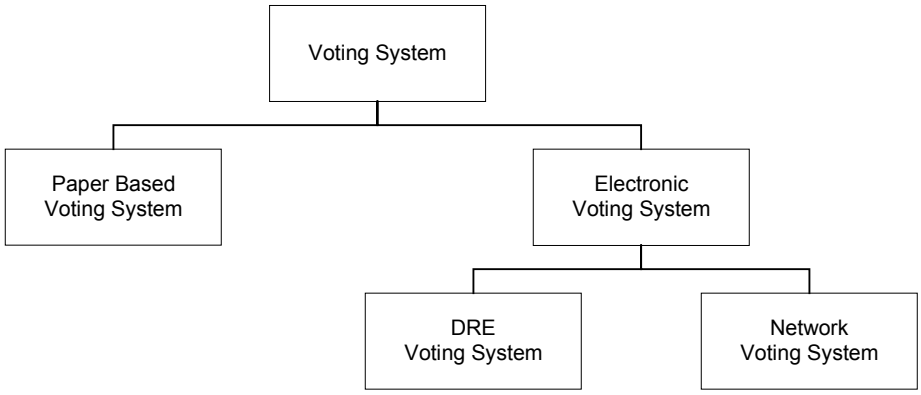
  > Other efforts label these systems as *Public Network Direct Recording Voting Systems*, or *Poll Site Internet Voting Systems*.

- *Unattended Network Voting Systems*. An Unattended Network Voting System is one in which one or more of the steps leading up to vote casting (voter identification, authorization, vote casting itself) take place in an environment that is not under the control or observation of election officials.

  > This type of system has been elsewhere labeled *Remote Internet Voting or Kiosk Internet Voting*.

- *Adjunct Network Voting Systems*. An Adjunct Network Voting System provides network system functionality to only a portion of the election process, and relies on other types of voting systems to perform the remainder of the election. These systems shall adhere to the portions of these standards applicable to the functions they provide.

The relationship between these different types of voting systems is represented in the following diagram:



Voting System Taxonomy

1.4. Intended Application of the Standards

At the time of this writing, the FEC is also in the process of revising their Voting System Standards. That effort includes standards for Public Network Direct Record Electronic Voting Systems, but explicitly excludes specifying standards for other online or network voting systems outside the attended poll site environment. These Network Voting System Standards are offered:

1. As both an alternative and as input to the FEC effort as it relates to any voting system that includes network connected voting devices, and

   The standards included in this document are based on a different model for establishing election validity than that followed by the FEC. The model underlying these standards results in standards that are less prescriptive yet more rigorous than those proposed by the FEC. The FEC standards for Public Network DRE Voting Systems are likely to prove insufficient to successfully protect the critical election requirements.

2. To ensure that upcoming trials (e.g., for military personnel and their dependents) of Network Voting Systems are conducted using systems that have been evaluated and demonstrated to meet a set of standards sufficient to protect the integrity of the elections.

2. Functional Requirements and Standards

2.1. Scope

This section contains the functional requirements and standards applicable to Network Voting Systems. Unless otherwise noted, these standards shall be met by all Network Voting Systems without regard to specific architectural division between hardware, firmware and software, underlying technology, or implementation methodology. *[FUNC-001]*

2.2. Organization

These standards are organized around the four fundamental requirements for all voting systems: fairness, accuracy, privacy and proof.

- **Fairness** – The system must allow all who are qualified to participate in the election that opportunity according to the rules and laws governing the election, and must *prevent* all who are not qualified from impacting the final tally. Fairness also speaks to the requirement that

the system enforce the rules governing the level of influence over the eventual tally granted to each participant

- **Accuracy** – The system must be able to accurately capture, preserve and tabulate the intent of the voters.

> Other discussions on this topic sometimes differentiate between "accuracy" and "data integrity". In these discussions, accuracy refers only to a system's ability to process a set of data without error, and data integrity refers to the system's ability to protect the data set from unauthorized change. In these standards, however, this differentiation is not made, and total system accuracy includes both concepts.

- **Privacy** – The system can not reveal any more information about how a particular voter voted than is revealed by the tally itself.

- **Proof** – The system must, without violating the privacy requirement, be able to prove that the fairness and accuracy requirements have been met.

> These fundamental requirements lead to a natural organization of the standards that is different from that of the FEC VSS. However, the requirements from the FEC VSS (security, accuracy and integrity, system audit, etc.) are addressed in these standards, in the context of how they contribute to these more fundamental objectives.

3. Fairness

The general fairness objectives for all election systems are to:

- Ensure only valid registered voters are allowed to vote;
- Ensure all valid registered voters are allowed to vote;
- Ensure that voters can vote on exactly the issues and races they are entitled to;
- Ensure that only one ballot is tabulated for each valid voter who voted.

The following sections describe the functional requirements and standards that Network Voting Systems shall meet to ensure that they are able to meet these fairness general objectives.

3.1. Ballot Preparation

Ballot Preparation is the process of defining the specific contests, questions, and related instructions to be contained in the ballots. It includes *Ballot Definition*, *Ballot Formatting,* and *Ballot Approval*. *Ballot Preparation* is fundamentally concerned with fairness, as the questions presented to each voter are based in large part on the preparation of the Ballot Styles for the election.

> What is labeled *Ballot Definition*, the FEC VSS calls *Election Programming*. This older label derives in large part to the need to program the punch card and op scan tabulation devices to scan and interpret the ballots. These standards utilize a more technology neutral label for the practice.

3.1.1. Ballot Definition

Ballot Definition is the process whereby election officials or their designees define the logic of the ballot(s). All Network Voting Systems shall provide for[8]:

a) The definition of elections, including the logical definition of political and administrative subdivisions as they affect ballot content and organization; *[BDEF-001]*

[8] Derived directly from VSS, Sections 2.3.1.2 and 2.3.2

b) The creation of ballot style(s) defining the collection(s) of offices, candidates, and measures on which the voters are entitled to vote by reason of place of residence, party affiliation, or other such administrative or geographical criteria; *[BDEF-002]*
c) A verifiable method to transfer the logical definition of the ballot(s) to those portions of the system responsible for verifying the correctness of the voter selections and for tabulating those selections. *[BDEF -003]*

All Network Voting Systems shall be capable of [9]:

d) Supporting at least 500 potentially active voting positions; *[BDEF -004]* and
e) Collecting and maintaining the following data:
    1. Offices and their associated labels and instructions; *[BDEF-005]*
    2. Candidate names and their associated labels; *[BDEF-006]* and
    3. Issues or measures and their associated text. *[BDEF-007]*

Finally, the Technical Data Package accompanying the system shall specifically identify which of the following voting options can be accommodated by the system[10]: *[BDEF-008]*

- Closed primaries;
- Open primaries;
- Partisan offices;
- Non-partisan offices;
- Write-in voting;
- Primary presidential delegation nominations;
- Candidate or answer rotation;
- Straight party voting options;
- Cross-party endorsement;
- Split precincts;
- Vote for N of M;
- Recall issues, with options;
- Overvotes;
- Undervotes; and
- Totally blank ballots.

3.1.2. Ballot Formatting

Ballot Formatting is the process whereby election officials or their designees designate how the specific contests and related instructions contained in the ballot are visually presented in a layout as permitted by the jurisdiction's election code. All Network Voting Systems shall provide a capability for the[11]:

a) Uniform allocation of space and fonts used for each office, candidate, and contest such that the voter perceives no active voting position to be preferred to any other; *[BFOR-001]*
b) Simultaneous display of all choices for a single contest on the same page, with no splitting across multiple pages or displays; *[BFOR-002]*
c) Easy navigation of multi-page ballots by voters, with no way to leave the balloting process unintentionally; *[BFOR-003]*

[9] Derived directly from VSS, Section 2.3.1.1.1
[10] Derived directly from VSS, Section 2.2.6
[11] Derived directly from VSS, Section 2.3.1.2

The layout of the ballot shall preclude the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system. (i.e., no potential for display of external information or linking to other information sources).[12] *[BFOR-004]* For Unattended Network Voting Systems, this requirement shall not preclude the voter from utilizing capabilities on their chosen voting device, yet outside the voting system itself, to access the aforementioned unauthorized information.

3.1.3. Ballot Approval

Ballot Approval is the process whereby election officials or their designees review and approve the correctness of the results of the *Ballot Definition* and *Ballot Formatting* stages of *Ballot Preparation*. In other words, election officials are reviewing and approving Ballot Styles. All Network Voting Systems shall provide a capability for:

a) The review of all attributes of the Ballot Styles(s), including ballot logic, layout, and languages. *[BAPP-001]*
   - For Attended Network Voting Systems, this review shall take place utilizing the same hardware and software environment as is present in the voting devices.
   - For Unattended Network Voting Systems, this review shall take place on the minimally capable hardware and software platform supported by the Network Voting System.

b) Ensuring the accuracy of any physical alignment required between the display of the Ballot Style and the device(s) used by a voter to indicate his or her preference(s). *[BAPP-002]*

c) An auditable irrefutable approval of the Ballot Style, such that the approval can be publicly verified at any time by other components in the system or by independent parties with the proper tools and knowledge. *[BAPP-003]* Once this approval has been granted, the system shall detect any subsequent changes to the ballot style and require the Ballot Style to be approved again. *[BAPP-004]*

3.2. Voter Declaration, Identification and Authorization[13]

This portion of an Network Voting System is concerned with correctly identifying and authorizing a registered voter to vote using the Network Voting System. This process is broken into three distinct steps: *Voter Declaration*, *Voter Identification*, and *Voter Authorization*.

> Note that in some circumstances, these steps may not be taken strictly in this order. For instance, in provisional voting, Voter Authorization takes place before Voter Identification is confirmed. The system is required to ensure all of these conditions are satisfied before a vote is included in the tally regardless of chronological order.

3.2.1. Voter Declaration

In the *Voter Declaration* process, registered voters declare their intent to vote in an election using a particular voting system.

Unattended Network Voting Systems shall require a request from the voter to vote using the system.

[12] Derived from VSS, Section 2.3.1.3 and 2.4.3.3

[13] Requirements and standards relating to what is commonly known as Voter Registration are outside the scope of these Network Voting System Standards.

[VDEC-001] This request shall contain voter identification information sufficient to legally identify the request as having originated from and been authorized by the voter, according to the laws and requirements of the jurisdiction conducting the election. *[VDEC-002]*

For qualified voters, the voter identification information shall be retained by the system for use during the *Voter Identification* phase. *[VDEC-003]*

3.2.2. Voter Identification

In the *Voter Identification* process, the voter presents his or her voter identification information in order to receive authorization to vote.

In Attended Network Voting Systems, the attendants are responsible for performing voter identification using traditional methods or information available to them as prescribed by jurisdiction law or convention. *[VIDN-001]*

In Unattended Network Voting Systems, the identification information shall enable unique and legally binding identification (according to the laws of the jurisdiction conducting the election) of the voter among all the voters that have been determined to be qualified to vote using the system during the *Voter Declaration* phase. *[VIDN-002]*

The system shall use this identification information to look up the voter's eligibility based on the determination made by the election officials during the *Voter Declaration* phase. *[VIDN-003]*

3.2.3. Voter Authorization

In the *Voter Authorization* process, election officials or their designees authorize a particular voter to cast a ballot in the election. This authorization may occur before the ballot is cast or, for those jurisdictions that provide for provisional or "fail-safe" voting, after the ballot is cast.

Network Voting Systems that include electronic ballot casting capabilities shall provide each authorized voter with unique credentials that can be audited to prove that only ballots cast by authorized voters have been included in the tally. *[VAUT-001]* The ultimate responsibility for determination of voter authorization shall remain with the election officials or their designees.

3.3. Accessibility

Network Voting Systems that provide ballot casting capabilities on components provided by the jurisdiction specifically for voting (includes Attended Network Voting Systems and Unattended Network Voting at jurisdiction provided kiosks, etc.) shall include capabilities for those portions of the system with which voters interact that meet the accessibility requirements for poll site voting equipment.[14] *[ACCS-001]*

Unattended Network Voting Systems shall include support for the accessibility features and capabilities included in the underlying hardware and software systems that are supported by the components of the voting system with which voters interact directly. *[ACCS-002]*

[14] FEC VSS – 2001 Update. Volume I, Section 2.2.7

3.4. Availability

The inclusion of network voting capabilities into any voting system shall not negatively affect any voter's ultimate ability to cast a valid ballot in the election. *[AVAL-001]*

> Many factors contribute to the total availability of voting systems. Some, including reliability, capacity, and maintainability, are directly related to design and manufacturing decisions made by the vendor. Others, including failures due to electrical power availability, physical or logical failure in one or more components, electrostatic susceptibility, and radio frequency or magnetic field interference, can be mitigated in the design, but are ultimately determined by the environment in which the system is deployed. Finally, there are those brought on by specific or malicious exploitation or attack of the system based on its design or implementation. For Network Voting Systems, these factors include the potential for denial of service attacks focused on connectivity or networking components or on the centralized portions (for those systems that include a 'data center') of the system itself.

For Attended Network Voting Systems, the baseline for availability comparisons shall be the total availability provided by other electronic poll site voting systems. *[AVAL-002]*

For Unattended Network Voting Systems, the baseline for availability comparisons shall be the total availability provided by other absentee voting systems. *[AVAL-003]*

The vendor of the Network Voting System shall prepare an Availability Analysis as a part of the Technical Data Package that describes the design and capabilities of the system with respect to meeting this requirement. *[AVAL-004]*

> Although these standards do not prescribe the solution, it is likely that to meet this standard most near-term network voting solutions will need to provide some form of fall back or fail-safe operating mode to ensure voting can still take place in the event of catastrophic equipment or telecommunications failure.
>
> As described in section 13, *Testing of Network Voting Systems*, the design review phase of system testing is critical to determining if a particular system design does or does not meet the availability requirements set forth in these standards.

3.5. One Voter – One Vote

All Network Voting Systems that include ballot tabulation capabilities shall limit each voter authorization to at most a single ballot in each tally. *[OVOV-001]*Those Network Voting Systems that deliver voted ballots to external tabulation systems shall provide either:

a) A capability to ensure only a single voted ballot for each voter authorization is delivered to the tabulation system; *[OVOV-002]* or
b) Enough information associated with each ballot that an external decision process might be employed to ensure that only a single ballot is tabulated for each voter authorization while maintaining voter privacy. *[OVOV-003]*

4. Accuracy

As defined in the FEC VSS[15]:

> *Voting system accuracy addresses the accuracy of data for each of the individual ballot positions that could be selected by a voter, including the positions that are not selected. For a voting system, accuracy is defined as the ability of the system to capture, record, store, consolidate and report the specific selections and absence of selections, made by the voter for each ballot position without error.*

[15] FEC VSS – 2001 Update. Volume I, Section 3.2.1

Like the FEC Voting System Standards, these standards recognize that each step in processing the vote data has the potential to introduce inaccuracies into the tally results. The model used to analyze this potential breaks the processing path down into the following steps:

- Recording the vote data,
- Transmitting the vote data,
- Storing the vote data,
- Confirming the accuracy of the vote data,
- Storage and preservation of the vote data,
- Tabulating the vote data, and
- Consolidation and Reporting of the tabulated data.

Each of these steps is examined in detail below.

The vendor shall prepare and submit an Accuracy Analysis as a part of the Technical Data Package. The focus of this document shall be to outline the system's approach to ensuring, preserving and proving accuracy at each step in the process. The Accuracy Analysis shall include documentation on the steps taken to preserve data integrity as well as the steps taken to confirm accuracy in data processing. *[ACCR-001]*

Network Voting Systems shall be tested against and meet at least the minimum standards for accuracy as described in the FEC VSS 2001 Update, section 3.2.1. *[ACCR-002]*

4.1. Vote Recording

The *Vote Recording* requirements for Network Voting Systems address the detection and recording of votes, including the logic and data processing functions required to determine the validity of voter selections, to accept and record valid selections, and to reject invalid selections.[16]

Network Voting Systems that include vote-recording capabilities shall[17]:

a) Except for provisional voters for whom the determination may not yet be made, enable election officials to control the selection of the Ballot Style presented to the voter, including limiting the voter's access to only those portions of the ballot upon which the voter is entitled to vote; *[VREC-001]*
b) Confirm the origin, authenticity, and integrity of the voter's blank Ballot Style subsequent to its approval by the jurisdiction; *[VREC-002]*
c) Confirm the capabilities and current operating mode of the voting device is consistent with those under which the Ballot Style was approved – to the extent that the ballot layout presented to the voter is consistent with the ballot layout requirements of the jurisdiction; *[VREC-003]*
d) Allow the voter to select his or her preferences on the ballot in any legal number and combination; *[VREC-004]*
e) Indicate a selection has been made or canceled; *[VREC-005]*
f) Indicate to the voter when no selection, or an insufficient number of selections, has been made in a contest; *[VREC-006]*
g) Prevent the voter from over-voting; *[VREC-007]*
h) Verify the correctness of the voter selections according to the *Ballot Definition* data approved by the jurisdiction; *[VREC-008]*
i) Record the selection and non-selection of individual vote choices for each contest and ballot measure; *[VREC-009]*

[16] Derived from FEC VSS – 2001 Update. Volume I, Section 3.2.1
[17] Derived in part from FEC VSS – 2001 Update, Volume 1, Sections, 2.4.2, 2.4.3, 3.2.4.3

j) Record the voter's selection of candidates whose names do not appear on the ballot, if applicable under jurisdiction law, and record as many of these 'write-in' votes as the number of candidates the voter is allowed to select; *[VREC-010]*
k) Record the permissible selections correctly; *[VREC-011]*
l) Notify the voter when the selection of candidates and measures is completed; *[VREC-012]*
m) Allow the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast; *[VREC-013]*
n) Prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and requiring the voter to confirm the voter's intention to cast the ballot; *[VREC-014]*
o) Prepare the ballot for transmission and storage as necessary to meet the requirements for Vote Preservation as described in Section 4.5; *[VREC-015]*
p) Notify the voter after the vote has been (transmitted and) stored successfully that the ballot has been cast; *[VREC-016]*
q) Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image itself, and instruct the voter on what to do should this event occur. *[VREC-17]*

4.2. Vote Transmission

The *Vote Transmission* requirements for Network Voting Systems address the transmission of vote data across public or private telecommunications or data networks. These standards shall apply to vote data transmitted as individual ballots and as collections or batches of ballots. *[VTRN-001]*

Network Voting Systems that include vote data transmission capabilities shall [18]:

a) Ensure all vote data is not altered during transmission; *[VTRN-002]*
b) Not disclose the content of the ballot, or in any other way violate or require the voter to relinquish privacy, during transmission; *[VTRN-003]*
c) Provide the voter or operator with clear indication of the success or failure of transmission and, in the case of failure, further provide the voter or operator with descriptions of corrective or alternative actions that should be taken. *[VTRN-004]*

4.3. Vote Storage

Network Voting Systems shall store vote data such that:

a) There is no single point of failure, logical or physical, which would lead to an unrecoverable loss of vote data; *[VSTR-001]*
b) The vote data can be irrefutably proven to have remained unchanged since being confirmed and cast by the voter. *[VSTR-002]*

4.4. Vote Confirmation

Vote Confirmation provides the voter an assurance that the vote data was recorded, transmitted and stored as originally intended by the voter. Network Voting Systems that provide electronic ballot recording, transmission, and/or storage capabilities shall:

a) Provide the voter with the ability to confirm that the vote data recorded, transmitted and stored by the system is an accurate representation of the voter's intent after it has been recorded, transmitted, and stored; *[VCNF-001]*
b) Provide Vote Confirmation capability without directly discovering or disclosing the content of the ballot to any portion of the system, or in any other way violating or requiring the voter to relinquish privacy; *[VCNF-002]*
c) Provide a means to allow the voter to correct the vote data if Vote Confirmation shows that vote data does not accurately reflect the voter's intent. *[VCNF-003]*

This capability provides the fundamental answer to questions about the trustworthiness of the machines on which the voting takes place. These questions are frequently referred to as the "client trust" issue. A voter who can be satisfied that the system, no matter what software

[18] Derived from FEC VSS – 2001 Update. Volume I, Section 2.2.10

(whether malicious or not) might be running, has been able to accurately capture, transmit, and store his or her intent no longer needs to merely trust the system to have done so.

4.5. Vote Preservation

Vote Preservation requires that the Network Voting System prevent any successful attempt at changing the collected vote data before, during, or after tabulation. Network Voting Systems that provide transmission and/or storage of electronic vote data shall:

a) Prevent and detect the addition of unauthorized vote data (voted ballots) into the tabulation process; *[VPRS-001]*
b) Prevent and detect the unrecoverable deletion of vote data (voted ballots), once receipt of such data has been confirmed to the voter; *[VPRS-002]*
c) Prevent and detect the unrecoverable modification of vote data (voted ballots), once receipt of such data has been confirmed to the voter; *[VPRS-003]*
d) Enable independent third party verification of these conditions without violating voter privacy. *[VPRS-004]*

These requirements may necessitate the redundant storage of ballot images, and/or the storage of ballot images on write-once media of some form, but in no case shall those measures be deemed sufficient by themselves to meet these requirements. Success in this context is fundamentally measured by the system's ability to prove that no possible changes to the vote data ultimately affected the accuracy of the tally.

4.6. Ballot Tabulation

All Network Voting Systems that provide Ballot Tabulation capabilities shall:

a) Prevent tabulation of the ballots before the balloting period has concluded and the polls are closed; *[BTAB-001]*
b) For ballots cast by provisional voters, enable election officials to ensure that the voters' influence on the final tally is limited to only those races or contests on which each voter is entitled to vote; *[BTAB-005]*
c) Accumulate votes, without error, from the authorized vote data according to the laws of the jurisdiction in which the election is taking place; *[BTAB-002]*
d) Provide complete accounting as to the disposition of all vote data confirmed received by the system, whether or not that data is included in the final vote tally. *[BTAB-003]*

The vendor of the Network Voting System shall identify in the Technical Data Package which of the voting options listed in Section 3.1.1, *Ballot Definition,* of these standards can be tabulated by the system. *[BTAB-004]*

4.7. Consolidation and Reporting

4.7.1. Consolidation[19]

All Attended Network Voting Systems that provide Ballot Tabulation capabilities shall provide a means to consolidate tabulation results data from all attended polling locations utilizing the system. *[CNSL-001]*

All Network Voting Systems that provide Ballot Tabulation capabilities shall provide a means to consolidate tabulation results data from other sources supported by the system as specified by the vendor, such as paper-based absentee voting systems, traditional poll site voting systems, and/or early voting systems. *[CNSL-002]*

[19] Derived from FEC VSS – 2001 Update. Volume I, Section 2.5.2

4.7.2. Reporting[20]

All Network Voting Systems shall:

a) Produce all system audit information needed to meet the requirements outlined in Section 6, *Proof*, of these standards; *[RPTG-001]*
b) Prevent data from being altered or destroyed by report generation; *[RPTG-002]*
c) Produce all reports in such a manner that their origin and integrity can be preserved and independently confirmed. *[RPTG-003]*

Further, all Network Voting Systems that provide Ballot Tabulation capabilities shall:

d) Provide geographic reporting, which requires the reporting of all results for each contest at the precinct level and additional jurisdictional levels; *[RPTG-004]*
e) Produce a report for each tabulator that includes:
   - the number of ballots counted, *[RPTG-005]*
   - the results of each contest including the votes cast for each selection, *[RPTG-006]*
   - the count of undervotes, and*[RPTG-007]*
   - for systems that are unable to prevent the submission of ballots that include overvotes, the count of each combination of overvotes (e.g., the number of overvotes combining candidate A and candidate B, combining candidate A and candidate C, etc.) and total overvotes; *[RPTG-008]*
f) Produce a report of the results as described above consolidated from all tabulators; *[RPTG-009]*
g) Produce reports that are completely consistent, with no discrepancy among reports produced at any level. *[RPTG-010]*

4.8. Security

This section describes essential security capabilities for Network Voting Systems. Voting system security requirements have traditionally focussed on securing access to an essentially closed environment – an environment where the election materials and vote data are always under the control of authorized officials. These traditional security standards are wholly insufficient for Network Voting Systems where the election materials and vote data regularly pass out of the direct control of the election officials.

Nevertheless, Network Voting System security must still meet the security objectives for all voting systems[22]:

- To establish and maintain controls that can ensure that accidents, inadvertent mistakes, and errors are minimized;
- To protect the system from intentional manipulation and fraud, and from malicious mischief;
- To identify fraudulent or erroneous changes to the system; and
- To protect secrecy in the voting process.

Since network elections take place in environments that are essentially impossible to close and control, security standards for this type of system must assume that all network processes and transactions are taking place in an open and uncontrolled environment. Therefore, Network Voting System security must be based on making the election data itself tamper-proof, rather than relying only on attempts to secure the processes and access to that data. *[SECR-001]*

[20] Derived from FEC VSS – 2001 Update. Volume I, Sections 2.5.3 and 3.2.6.2.2
[21] http://www.votehere.net/perspectives/DoVotingRight.pdf
[22] Derived from FEC VSS – 2001 Update. Volume I, Section 6.1

Specifically, any unauthorized changes to the election data must create an intrinsic inconsistency that is detectable by any thorough data audit. *[SECR-002]*

> This approach allows the election materials and vote data to be examined at any stage of the election necessary to determine if the election has been compromised by anyone or anything, without regard for whether the source of the compromise is known or unknown at the time of the voting system design, implementation, deployment, or use.

Network Voting Systems shall provide capabilities that prevent undetected, unauthorized changes to all election data maintained and/or produced by the system, including (depending on the scope of the capabilities of the specific system): *[SECR-003]*

- Voter authorizations and credentials;
- Approved Ballot Style information;
- Voted ballots;
- Vote tallies.

4.8.1. Penetration Analysis

Vendors of all Network Voting Systems shall provide an analysis of the systems' potential attack points. The analysis shall include known attack methods, risk and extent of potential damage, as well as deterrence, and prevention and mitigation approaches designed into the system. This analysis shall include potential vectors of system penetration due to elements and influences both inside and outside the control of the vendor and the jurisdiction officials. *[PENA-001]*

The Penetration Analysis and the information it contains shall be kept confidential and shall be disclosed only to those parties who need it to perform analysis of the system design and implementation.

4.8.2. Access Control[23]

For Network Voting Systems physical and logical access controls alone are insufficient to establish acceptable assurance of system integrity, for two reasons:

1. Such controls can not protect the election from those who have been granted sufficiently high access privileges; and
2. Such controls can not guarantee that other people or processes have not altered the election data.

However, access controls shall be included as a useful "first line" of defense against many possible penetration attempts. In addition, careful logging of access to controlled resources and systems can provide useful forensic evidence in the event the data security analysis indicates a failure of system integrity has occurred.

Access controls are procedures and system capabilities that detect or limit access to the system to help guard against loss of system integrity, availability, and accountability. Access controls may include physical controls, such as keeping computers in locked rooms to limit physical access, and technical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. The access controls contained in this section of the standards are limited to those required of system vendors and do not extend to the access controls required of jurisdictions.

All Network Voting Systems shall provide access control capabilities including:

a) Identifying individuals to whom system access is granted; *[ACTL-001]*
b) Identifying any limits of access granted to each individual, including time, specific function, and/or data as appropriate to the system; *[ACTL-002]*
c) Granting authorized access to individuals based on their access privileges; and*[ACTL-003]*
d) Denying access to a function and/or data to unidentified individuals; *[ACTL-004]*

[23] Derived from FEC VSS – 2001 Update. Volume I, Section 6.2

e) Denying access to a function and/or data to identified but otherwise unauthorized individuals. *[ACTL-005]*

The Technical Data Package for all Network Voting Systems shall include recommended policies for effective implementation and maintenance of the access control capabilities included in the system. *[ACTL-006]* These recommendations shall include all of the following topics as dictated by the specifics of the system design and implementation:

a) Use of included hardware and/or software access controls; *[ACTL-007]*
b) Effective password or access key management; *[ACTL-008]*
c) Recommended segregation of authorized duties; and*[ACTL-009]*
d) Any other relevant characteristics or parameters. *[ACTL-010]*

Vendors shall define and provide a detailed description of the methods used to preclude unauthorized access to the access control capabilities of the system itself. *[ACTL-011]*

4.8.3. Physical Security

All Network Voting System vendors shall develop, provide, and document measures to limit physical access and threats to the system components under the control of the jurisdiction and system vendor. *[PSEC-001]*

Meeting this requirement shall not eliminate the need to fulfill the requirements of section 6, *Proof*, in these standards.

4.8.4. Telecommunications

All Network Voting Systems shall be designed to maintain the security and privacy of all transmitted election data in a telecommunications environment that is assumed to be publicly or privately accessible and monitored. *[TCON-001]*

Specifically, these systems shall presume that all transmissions are subject to monitoring by parties other than the intended recipient, and shall in any case prevent unauthorized modification, discovery, or disclosure of election data. *[TCON-002]*

> Some networks may claim better physical and/or logical security than this. There is no reason, however, to rely on the physical security of the link itself, which only pushes the problem of preserving the security and privacy of the data to the end points of the communication, and opens an attack vector should the physical security of the network ever be violated.

5. Privacy

Privacy is the requirement that the system can not reveal any more information about how a particular voter voted than is revealed by the tally itself. While this is the abstract objective for privacy in all election systems, different levels of voter privacy are provided in different voting systems based on their design and underlying principles. These differences can be categorized into these general models (in order of increasing general 'strength' or capability):

- Trusted Authority – The privacy and integrity of the vote data is protected only by some trusted individual or organization (presumably because they have no vested interest in the outcome). In this model, the election results themselves cannot be independently audited without also violating privacy. Systems relying on a trusted authority model to protect election integrity or privacy do not meet the minimum level required in these standards.

- Threshold Privacy – The privacy and integrity of the vote data is protected by some number of trusted individuals that must act together to process the information. Effective threshold

privacy is dependent on distributing the trust among enough individuals that their interests not likely to align strongly enough to invite collusion.

- Computational Privacy – The privacy and integrity of the vote data is protected by secret information held by the voters themselves. This level of protected can be defeated only through brute force attack on the secrecy of the data itself.

- Absolute or Information Theoretic Privacy – The association between the voter and his or her ballot does not exist in the system.

Traditional mechanical, paper-based and electronic poll site voting systems are generally thought to provide this level of privacy, although in practice, because there are people involved in the process, a strict analysis of the system often reveals that these systems provide threshold privacy, and are sometimes even providing only trusted authority levels of assurance.

Network Voting Systems shall provide at least threshold privacy.[24] *[PRIV-001]* Threshold Privacy capabilities shall include:

a) Enabling the jurisdiction to specify the threshold number of trusted individuals that must concur and act intentionally before any processing of vote data takes place; *[PRIV-002]*
b) Except in the event of cooperative disclosure by at least the threshold number of trusted individuals, preventing the disclosure of more information about how any particular voter voted than is revealed by the tally itself; *[PRIV-003]*
c) Requiring the trusted individuals to identify themselves to the system using technology at least as irrefutable as that used to identify authorized voters in the system; *[PRIV-004]*

Network Voting Systems shall include provisions to prevent automated (that is all approaches that require no in-person interaction with the voter) voter coercion and vote selling. *[PRIV-006]*

Network Voting System vendors shall submit a Privacy Analysis as a part of the Technical Data Package, which details the design and capabilities of the system specifically included to meet the privacy model specified by the vendor. This privacy analysis shall also include descriptions of the provisions included in the system to prevent automated voter coercion and vote selling. *[PRIV-007]*

6. Proof

Election audit trails provide the supporting documentation for verifying the correctness of reported election results. They present an archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation.[25]

[24] Requirement derived from the report of the California Internet Voting Task Force Report, Section 10.
[25] Derived from FEC VSS – 2001 Update. Volume I, Section 2.2.5.1

Traditionally, the need to preserve privacy has focused election system audit on the creation and maintenance of activity and event logs – auditing the election *process*. At best, these *process audits* can only *imply* quality of the election data, and thus the validity of the election data. In the relatively uncontrolled and open environment in which network voting takes place, it is difficult to prove that all possible influences on the election materials and vote data had been monitored and audited appropriately. Therefore, the inferred indications of quality provided by process audits alone shall not be sufficient in Network Voting Systems. In their place, Network Voting Systems shall provide capabilities that allow for a complete audit of the election data itself. The direct examination of the integrity and validity of the election data itself removes the uncertainty that it was somehow modified and invalidated in process or in transit.

All Network Voting Systems shall produce a complete *transcript* of all election data required to determine the validity and consistency of the election results. *[PROF-001]*

The system shall enable anyone to independently examine and verify the validity and correctness of the transcript without violating the privacy requirements of these standards. *[PROF-002]*

All Network Voting Systems shall maintain an event log containing audit records to be relied upon only for forensic discovery in the event the audit of the election data indicates possible discrepancies or violations of data integrity. *[PROF-003]*

The details of each of these parts of the election audit data are described in the following sections.

6.1. Election Data Transcript

The Election Data Transcript is the key to protecting and assuring the validity of elections conducted using Network Voting Systems. An audit trail of all processes and people that have come in contact with or affected the election data in known ways shall not be sufficient to satisfy this requirement.

All Network Voting Systems shall produce transcripts of election data. *[TRAN-001]*

The Election Data Transcript shall include sufficient information generated throughout the election that it is impossible to forge a valid data transcript with data other than that actually created during the election. *[TRAN-002]*

At a minimum, the Election Data Transcript shall enable independent, irrefutable verification that:

a) All specific assumptions and properties about technology specific data (such as encryption key quality, randomness, and others qualities as appropriate to the system specific design and implementation) are valid; *[TRAN-003]*
b) All election parameters, Ballot Styles, and other critical pre-election data were approved by a known and authorized individual; *[TRAN-004]*
c) All voter authorizations were issued by a known and authorized individual; *[TRAN-005]*
d) All ballots can be tied to valid voter authorizations for the election; *[TRAN-006]*
e) Only a single ballot for each valid voter authorization is included in the tally; *[TRAN-007]*
f) All voted ballots were voted on approved Ballot Styles; *[TRAN-008]*
g) All voted ballots follow the rules of the appropriate approved Ballot Style Definition; *[TRAN-009]*
h) All voted ballots were cast in accordance with the approved election parameters, including polling times, privacy parameters, and others as appropriate to the system specific design and implementation. *[TRAN-010]*
i) No ballots have been modified since they were cast and confirmed by the voter; *[TRAN-011]*
j) All ballots for which the system has acknowledged receipt to a voter are accounted for, but may be segregated by disposition (for example, test ballots, provisional ballots, bad ballots, or others as appropriate to the specific system design and implementation); *[TRAN-012]*
k) The election results accurately reflect the data contained in all ballots from valid voter authorizations, as appropriate based on the system design and jurisdiction policy; *[TRAN-013]*
l) The transcript itself has been generated by a known and authorized individual, and has not been modified since it was generated. *[TRAN-014]*

The vendor shall clearly specify in the Technical Data Package the formats and conventions used in the data transcripts, and shall enable independent verification procedures and/or processes to be developed from this information. *[TRAN-015]*

Network Voting Systems that do not provide complete voting system functionality need only produce transcripts consistent with the election data that they do process or convey.

The Network Voting System shall provide capabilities to produce printed records of all transcript data, including the voted ballots, in human readable form. *[TRAN-016]*

6.2. Election Event Log

The Election Event Log shall not be used alone to establish election validity. The determination of final election validity for elections held using Network Voting Systems shall be based on the review and analysis of the Election Data Transcript.

All Network Voting Systems shall maintain a system-generated set of audit records of major events that take place during the process of the election. *[EVNT-001]*

Because the actual implementation of specific characteristics may vary from system to system, the vendor shall describe each system's characteristics in sufficient detail that ITAs and system users can evaluate the adequacy of the system's audit trail.[26] *[EVNT-002]*

This evaluation shall focus on the event log's use as a forensic tool in determining the source or cause of any compromise of the election as indicated by the election data audit. *[EVNT-003]*

6.2.1. General Requirements[27]

All Network Voting Systems shall meet the following requirements for time, sequence, and preservation of audit records:

a) Systems shall provide the capability to create and maintain a real-time audit record; *[EGEN-001]*
b) All systems shall include a real-time clock as part of the system's hardware. The system shall maintain an absolute record of the time and date or a record relative to some event whose time and data are known and recorded; *[EGEN-002]*
c) All audit record entries shall include the time-and-date stamp, and wherever possible without violating voter privacy, the identity of the individual or individuals performing the operation; *[EGEN-003]*
d) The audit record shall be active whenever the system is in an operating mode. This record shall be available at all times, though it need not be continually visible; *[EGEN-004]*
e) The generation of audit record entries shall not be terminated or altered by program control, or by the intervention of any person. The physical security and integrity of the record shall be maintained at all times; *[EGEN-005]*
f) Once the system has been activated for any function, the system shall preserve the contents of the audit records during any interruption of power to the system until processing and data reporting have been completed; *[EGEN-006]*
g) The system shall preserve a copy of the audit records in printable form. *[EGEN-007]*

The requirement to generate and store audit event log entries shall not extend to system components outside the control of the jurisdiction and the system vendor.

[26] Derived from FEC VSS – 2001 Update. Volume I, Section 2.2.5.1
[27] Derived from FEC VSS – 2001 Update. Volume I, Section 2.2.5.2.1

6.2.2. Event Log Entries[28]

The event log requirements listed in the following subsections are considered essential to a complete forensic recording of the election process. This list of events may not reflect the design constructs of some systems. Therefore, vendors shall supplement it as appropriate with information relevant to the operation of their specific systems. *[ELEN-001]*

6.2.2.1. Pre-election Event Records

The following pre-election event records shall be logged at a minimum:

a) The approval of the final Ballot Styles; *[ELPE-001]*
b) The approval of the final election parameters, including poll times, privacy parameters, and/or any other data as appropriate to the specific design and implementation of the voting system; *[ELPE-002]*
c) All transactions related to voter declaration and preparation of voter credentials, as appropriate to the specific design and implementation of the voting system; *[ELPE-003]*
d) All transactions related to the readiness and accuracy testing of the system and the specific election parameters, including the expunging of test data as appropriate or required by the specific design and implementation of the voting system. *[ELPE-004]*

6.2.2.2. In-Process Event Records

In-process event records document system operations during the casting and tallying of ballots. At a minimum, the in-process event records shall contain:

a) Machine generated error and exception messages to demonstrate successful recovery. Examples include, but are not necessarily limited to:
    1) The source and disposition of system interrupts resulting in entry into exception handling routines; *[ELIP-001]*
    2) All messages generated by exception handlers; *[ELIP-002]*
    3) The identification code and number of occurrences for each hardware and software error or failure; *[ELIP-003]*
    4) Notification of system login or access errors, file access errors, and physical violations of security as they occur, and a summary record of these events after processing; *[ELIP-004]*
    5) Other exception events such as power failures, failure of critical hardware components, data transmission errors, or other type of operating anomaly. *[ELIP-005]*
b) Critical system status messages other than informational messages displayed by the system during the course of normal operations. *[ELIP-006]* These items include, but are not limited to:
    1) Diagnostic and status messages upon startup;
    2) Error messages and notifications as they are encountered during operation;
    3) All transactions related to operator access to the system, whether in normal or exceptional conditions;
c) All transactions related to the process of balloting; *[ELIP-007]*
d) The closing of the voting period / polls; *[ELIP-008]*
e) All transactions relating to the tabulation of the ballots and production of reports. *[ELIP-009]*

7. Hardware Standards

Network Voting Systems may be designed to run on entirely off-the-shelf (COTS) hardware, on proprietary hardware, or using a mix of proprietary hardware and COTS hardware.

7.1. Proprietary Hardware

Network Voting Systems that utilize vendor proprietary hardware, either in attended or unattended network voting scenarios, shall meet the functional characteristics and requirements described in these

[28] Derived from FEC VSS – 2001 Update. Volume I, Section 4.5 and sub-sections.

standards, and shall test and qualify the proprietary hardware components to the Design, Construction and Maintenance Characteristics[29] as described in the FEC Voting System Standards in force at the time of system qualification testing. *[HWPR-001]*

Subsequent modification to the proprietary hardware components of the system shall be evaluated to determine the scope of impact to the system, and shall result in re-testing as agreed upon the by the vendor and a qualified ITA. *[HWPR-002]*

7.2. Commercial Off-The-Shelf Hardware

Commercial off-the-shelf (COTS) hardware components refers to complete hardware systems or products, offered for commercial sale by vendors other than the vendor of the election system, and integrated into the complete voting system without modification.

COTS hardware components shall undergo functional and system level testing in the context of their integration into and testing of the voting system as a whole. *[HWCT-001]* COTS components shall not be required to undergo the Design, Construction and Maintenance characteristics testing so long as they have been granted approvals common to that particular type of equipment in industry (e.g., UL, FCC, etc.)

Qualification of COTS hardware components shall be performed and accepted on a 'minimum, or equivalent' basis, allowing vendors or jurisdictions to substitute COTS components of equivalent or superior functional capability into the system configuration without need for re-qualification. *[HWCT-002]*

The vendor of the Network Voting System shall clearly identify the minimum standards for the relevant characteristics of all COTS hardware included in the system. *[HWCT-003]*

The vendor shall submit a complete description of all COTS hardware substitutions that have been made between the time of system qualification and the time of system acceptance testing by a jurisdiction. This data shall include proof that the newer components meet at least the minimum functional capabilities of the system as originally qualified. *[HWCT-004]*

8. Software Standards

All Network Voting System software components shall meet the requirements of the FEC Voting System Software Design and Coding Standards[30] in force at the time of system qualification. *[SWRE-001]*

9. Telecommunication Standards

Telecommunications form the backbone of Network Voting Systems.

Whether over public or private telecommunication networks, and without regard for the particular telecommunications technology used, all Network Voting Systems shall maintain the integrity, accuracy, and privacy of all election materials and vote data transmitted over the communications link. *[TELE-001]*

There shall be no limitation on the types of election data that are transmitted as long as the vendor can show that these requirements are met for each data type.

10. Cryptographic Standards

Modern data cryptography offers tools and capabilities that may be useful in designing and implementing a Network Voting System that meets these standards.

[29] Volume I, Sections 3.2.2, 3.3 and 3.4 in the FEC VSS – 2001 Update
[30] Volume I, Section 4.2 in the FEC VSS – 2001 Update

Vendors who employ cryptographic approaches in their systems shall include a Cryptographic Analysis in the Technical Data Package. *[CRYP-001]* This analysis shall, at a minimum, enable a review of the cryptographic design and implementation to ensure that the system:

- Meets the requirements as described in these standards; *[CRYP-002]*
- Meets at least the generally accepted commercial norms and standards for implementation of cryptographic components (e.g., Common Criteria or ISO 15408, FIPS 140-X, etc.). *[CRYP-003]*

Note: specific industry standards will be identified in a future draft of these requirements.

11. Quality Assurance Standards

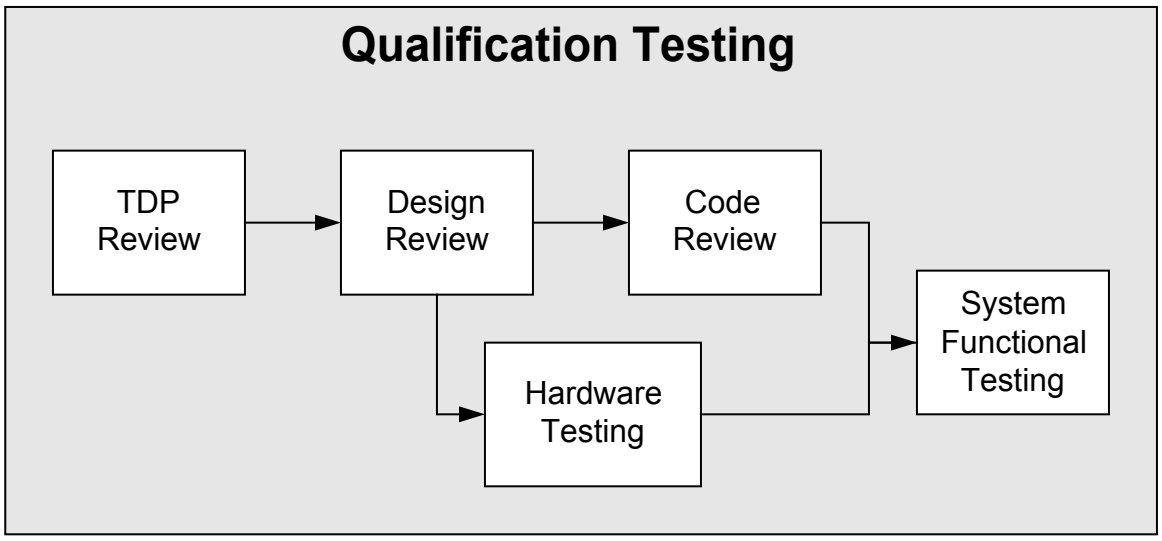
All Network Voting System components shall meet the requirements of the FEC Voting System Quality Assurance Standards[31] in force at the time of system qualification. *[QUAL-001]*

12. Configuration Management Standards

All Network Voting System components shall meet the requirements of the FEC Voting System Configuration Management Standards[32] in force at the time of system qualification. *[CONF-001]*

13. Testing of Network Voting Systems

Testing of systems to be measured against these standards shall take place following the process pictured in the following diagram:



13.1. TDP Review

The testing process begins with an examination and review of the Technical Data Package submitted by the vendor. The review shall ensure that the TDP contains all required components and information, and that the materials required to perform the subsequent design review are included. This review shall also include the vendor's Quality Assurance Program and Configuration Management Plan as documented in the TDP.

[31] Volume I, Section 7 in the FEC VSS – 2001 Update
[32] Volume I, Section 8 in the FEC VSS – 2001 Update

Note: details on the required content of the TDP will be forthcoming in a future draft of these requirements.

13.2. Design Review

These standards intentionally define requirements rather than specific functional designs. Before the functional testing specific to each system can be performed, a design review and analysis must be performed to determine if the system is logically able to meet the requirements of these standards. This design review shall focus on the content of the Capacity, Availability, Accuracy, Penetration, Privacy, and Audit Analysis portions of the TDP. This review shall also include the review of the detailed designs appropriate to the technology selected by the vendor (e.g., cryptographic protocol review and analysis for cryptography based systems, etc.).

The goal of a successful design review is a statement to the effect of: "If this system works as designed it will meet the standards.".

13.3. Hardware Testing

This testing shall focus on the operational and environmental testing of proprietary hardware components to ensure that they meet the requirements of these standards.

13.4. Code Review

This review is to determine if the proprietary source code components of the system have been designed and implemented in a fashion consistent with these standards.

13.5. System Functional Testing

This step in the testing process involves functional and performance testing of the integrated system, including tests covering the full scope of the functional requirements contained in these standards.

The goal of this phase of the testing is to verify the "if this system works as designed…" qualifier on the statement coming out of the design review.